



NORTH DALLAS ADVENTIST ACADEMY

2021-2022 TECHNOLOGY POLICY: GRADES K4-12

All students and all electronic devices (computers, tablets, cell phones, cameras, Smartwatches, and other music-playing and communication devices, etc.), whether student-owned or school-owned, are subject to the following acceptable use policies and procedures. These policies and procedures govern student use of electronic devices while at school and while on school-sponsored trips and events. School-owned devices are covered by this policy at all times and in all places.

North Dallas Adventist Academy embraces the appropriate use of electronics as a learning tool in our academic environments. School-owned electronic devices are intended to enhance learning while limiting overuse or distractions from superfluous personal electronic devices.

Student-owned personal electronic devices are not allowed to be used by students during the school day. They should be turned in at the front desk upon arrival. This includes, but is not limited to cell phones, computers, tablets, cameras, Smart watches, other music-playing devices, headphones/earbuds or any other device restricted by North Dallas Adventist Academy. This is applicable for all students.

Parents may apply for a technology acceptable use exception with documented medical conditions or documented learning differences, or for students participating in dual-credit courses.

Use of Computer Resources

The technology network and internet resources provided by the school for the use of its students are expressly for the purpose of advancing the educational mission of the school. Students should refrain from downloading or accessing videos, music, games, etc. Technology resources should not be used for personal, nonacademic purposes. The Academy reserves the right to monitor, access, intercept, retrieve, and/or read the entire content of any electronic message, document, telephonic, telefax (FAX) or voice mail communication transmitted to/from or stored in any school-owned device to the maximum extent permitted by law, including communications and computer data that have been deleted by users.

Note: The term "school-owned device" also applies to any off-campus storage device or company which the Academy uses for electronic storage.

Use of Personal Electronic Devices

Student's use of personal electronic devices, which includes but is not limited to cell phones, cellphones, Smartwatches, cameras, personal laptop computers, or tablets on campus or school-sponsored activities is governed by the school's acceptable use policy. Students have a responsibility to know and follow school guidelines regarding what is appropriate and permissible in this area. The school reserves the right to confiscate and examine the contents of students' personal communication device if there is reason to believe there is evidence of harassment, bullying, pornography, the transmission of sexual material/inappropriate pictures or videos, illegal activity, etc. Students who refuse to surrender their phone or to make the information accessible to us may be subject to further discipline, up to and including expulsion.

Student Cell Phones and Electronic Devices

Once students arrive on campus, they will be required to check-in their cell phones or any other electronic device with a designated staff member before entering their appointed school zone. When they leave campus, they will need to sign-out their devices from the designated staff member as well. During the day, the devices will be kept locked in a protective cabinet in a particular slot assigned to the individual student. If a student is found to be in possession of or use of a cell phone or an unauthorized electronic device, the device will be confiscated and delivered to the Principal.

Electronic Communication

Correspondence via electronic communication on North Dallas Adventist Academy's network or on personal electronic devices during school hours is to be used primarily for education and administrative purposes. The content of electronic messages, documents, and/or images must conform to the Academy's ethical and educational standards. The use of profanity, vulgarity, ethnic, or racial slurs, and other inflammatory language in any communication is prohibited. Electronic messages must not misrepresent the identity of the sender and should not be sent as chain letters, or broadcast indiscriminately. Electronic messages by students during school hours are not private and are monitored to ensure appropriate use.

If students receive any inappropriate or offensive electronic communications, students shall refrain from forwarding the communications to others and to notify a faculty/staff member immediately.

Any electronic communication (including video or images) sent by or to NDAA students and/or faculty/staff members which is contrary to the Academy's ethical and educational standards is strictly prohibited, regardless of whether the communication is sent on an Academy-owned or privately-owned device. If inappropriate communication is sent or received by academy students or faculty/staff members which is contrary to the Academy's ethical and educational standards, including, but not limited to any communication which includes the use of sexual, threatening or abusive language, profanity, vulgarity, ethnic or racial slurs, derogatory epithets, innuendos, or other inflammatory language, NDAA shall have the right to inspect any electronic device and the entire contents of the device, no matter if the device is on or off school property.

NOTE: The term "contents of the device" includes any physical or electronic information stored on the device.

Security and Confidentiality

NDAA implements, monitors, and evaluates both networked and non-networked devices, which includes but is not limited to personal electronic devices, electronic media resources for instructional and administrative purposes. This is done to ensure the appropriate and proper use of those resources. The Academy does not guarantee the security, accuracy, quality, or confidentiality of data accessed, prepared, stored, transmitted, or otherwise developed through the Academy. The Academy will not be responsible for any damages suffered as a result of an individual's use of the Academy's computer system or network, including the loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by the Academy's negligence, errors, or omissions.

Information prepared, stored, transmitted, or otherwise developed through NDAA, including but not limited to email transmissions, images, or videos shall not be considered private. The Academy may access individual files or activity logs at any time. All computer files students save or work on may not be kept confidential from students' parents/guardians.

User Responsibilities

- Students assume personal responsibility for the use of their network user account and are responsible for maintaining the security of the account. Students are prohibited from disclosing their network user password and from otherwise making the Academy's computer or network resources available to unauthorized individuals, including family and friends. Students' possession or collection of passwords, personal identification numbers, private digital certificates, or other secure identification information belonging to other users is prohibited. Use of another user account is prohibited.
- Students shall surrender their cell phone to the Main Office every time they enter campus, prior to proceeding into the building. Students may sign out their cell phone as they are leaving campus for the day. Students are not to keep cell phones in their lockers, backpacks, bags, or on their person during the school day.
- Students shall not deliberately use electronic devices to annoy or harass others with unacceptable language, images, or threats. Students shall not deliberately access unacceptable, obscene, or objectionable information, internet sites, language, or images. If such information is accessed, students must notify a faculty/staff member immediately. The Academy cannot completely protect students from accessing inappropriate materials and specifically denies any responsibility for students accessing inappropriate, offensive, illegal, or obscene materials.
- Use of the internet should be solely for academic purposes as directed by faculty/staff members. Students shall not reveal personal information about themselves. Students shall not arrange meetings with anyone met online. Students shall not enter any internet "chat rooms" unless authorized by faculty/staff. Any inappropriate use of the internet should be reported to a faculty/staff member immediately.
- Transmission of any material in violation of federal or state regulations is prohibited. Students shall not violate copyright laws or plagiarize the work of another. NDAA shall not be liable for students' inappropriate use of electronic communication resources, violations of copyright restrictions or other laws, students' mistakes or negligence, or costs incurred by students.
- Use of any Academy computer or network for commercial or political purposes is a violation of these terms and conditions of use.
- Students are prohibited from installing, storing, or using unlicensed or illegal copies of software on NDAA computers. Transmission of such software over the Academy's network is prohibited. Only the Academy IT Department is authorized to install or uninstall software on the Academy's computers and devices.
- Students may use only the computing resources for which they are authorized and only for the purposes specified.
- The introduction of data or programs which in some way endangers computing resources, or the information of other users, (e.g., a computer worm, virus, or other destructive code), or which infringes upon the rights of other Academy computer users (e.g., inappropriate, obscene, pornographic, bigoted, or abusive materials) is prohibited.
- Students may not attempt to circumvent security systems or to exploit or probe for security holes in any NDAA device, network or system, nor may students attempt any such activity against other systems accessed through the Academy's devices. Execution or compilation of programs designed to breach system security is prohibited.

- If students' personal electronic devices are encrypted and the Academy deems it necessary to inspect the devices, students must make all data available in an unencrypted format.
- The printing facilities of NDAA should be used sparingly. Unnecessary printing may result in the loss of printing privileges. There is a per page charge for printing any copies and must be paid to the Main Office prior to printing.
- Vandalism will result in cancellation of technology privileges and other disciplinary measures in compliance with NDAA policy and the discipline code. Vandalism includes any malicious attempt to access, copy, use, harm, or destroy data of another user, of the system, or of any of the agencies or other networks that are connected to the internet, and as the intentional damage or destruction of Academy-owned device, hardware, software or data.
- All hardware, software, peripheral equipment, data files, cabling, and programs are the property of the Academy.
- Access to NDAA's electronic computer system is a privilege, not a right. Students shall be required to acknowledge receipt of these policies. Students will be required to comply with these guidelines.
- These procedures, guidelines, and/or policies are subject to modification at any time.
- Any broken or damaged school-owned device should be reported immediately to the office. Students/parents are asked NOT to have repairs made without consulting with the Academic Office. NDAA holds AppleCare and any repairs done outside of this agreement may negate the AppleCare agreement. The student/parent would then be responsible for the repair and/or replacement of the device.

Social Networks

Social networking sites provide many positive opportunities for communication and connectivity. In keeping with the mission of NDAA, students are encouraged to use the social networking sites for the development and maintenance of healthy relationships. Students should refrain from making derogatory, defaming, threatening, or profane comments against fellow students, faculty/staff, and school. Students found to be posting such comments are subject to disciplinary action by NDAA's Discipline Committee.

Consequences and Violations

Any use of NDAA's computer resources which violates the Academy's policies and procedures involving the use of computers and networks may result in disciplinary action, including, but not limited to the Academy removing data and programs that are found to be inappropriate, terminating the computer privileges of the violating user, suspension, or expulsion. Administration will determine when a policy or procedure has been violated and the appropriate consequences.

In addition to violating NDAA policy, certain computer misconduct may be prohibited under state and/or federal law and may, therefore, be subject to criminal penalties. Such misconduct includes knowingly gaining unauthorized access to a computer system, illegally gaining access to data, causing a computer to malfunction, or interrupting the operation of a computer without the effective consent of the owner. Violators of such misconduct may be reported to appropriate law enforcement.

Student cell phones and/or personal electronic devices found to not be stored in the designated cell phone case will be immediately confiscated.

Student-owned personal electronic devices, including but not limited to computers, tablets, cameras, iPods, iWatches, music playing devices, headphones/earbuds or any other device must be powered off and turned in to be stored during school hours of 8:00 a.m. to 3:45 p.m.

Violation of student-owned personal electronic use policy results in the following procedure:

- **1st Offense:**
Complete cell phone/device will be confiscated, given to the School Principal for 24-hour hold, and a \$50 fine that must be paid before the device is returned. Device will be released with confirmation from Parent/Guardian. Demerit consequence: 20
- **2nd Offense:**
Complete cell phone/device will be confiscated, given to the Principal for 48-hour hold and a \$50 fine that must be paid before the device is returned. The student also receives one week of In-School Suspension (ISS). Parents/Guardians will be communicated with from the Principal's Office so that device will be released to parent/guardian only.
Demerit consequence: 30
- **3rd Offense:**
The student will be suspended for 3 days and will be required to meet with the Disciplinary Committee with a parent. Students will be fined \$50 and given 40 demerits. The student will no longer be allowed to bring his/her phone to school. Demerit consequence: 40

A student that refuses to comply with a request to surrender his/her cell phone or unauthorized electronic device by any member of the faculty or staff and/or administrator will be considered insubordinate and will be placed in ISS (in school suspension) immediately until review by administration.